

Datenschutzerklärung Westfalia Connect

1. Data Controller

Westfalia Mobil GmbH
Gleichenstraße 20
99867 Gotha
Germany

Data Protection Officer:
Sascha Hasselbach
Phone: +492173 20 41 244
Email: sascha.hasselbach@datenschutz-extern-nrw.de

2. General information on data processing

We process personal data exclusively within the framework of applicable data protection laws, in particular the General Data Protection Regulation (GDPR).

Personal data is any information relating to an identified or identifiable individual.

3. Categories of data processed

Technical data, vehicle data and communication data can be processed.

In the context of the use of the WebApp, the following data in particular may be processed:

a) Account data

- Name
- Email address
- Phone number
- Username
- Password (stored in encrypted form)

b) Technical data

- IP address
- Browser Type
- Operating System
- Device Information
- Language settings
- Access times

- Log data
- c) Vehicle and on-board data
- Vehicle Identification Number (VIN)
 - Device status
 - Battery status
 - Tank or state of charge
 - Temperature values
 - Location data (if enabled)
 - Diagnostics and error messages
 - Usage data of the on-board functions
- d) Communication data
- Support Requests
 - Chat or service messages
 - Feedback messages

4. Purposes of processing

The processing is carried out for the provision of the web app, for authentication and for the control of on-board functions.

The processing is carried out in particular for the following purposes:

- Provision of the WebApp,
- Managing user accounts,
- Carrying out authentications,
- Control and management of on-board functions,
- Error analysis and system safety,
- Improving services,
- Providing support services,
- Compliance with legal obligations.

5. Legal basis

The processing is carried out on the basis of the GDPR, in particular Art. 6 para. 1 lit. a, b, c and f GDPR.

The processing of personal data is carried out on the basis of:

- Art. 6 (1) (b) GDPR (performance of a contract),
- Art. 6 (1) (c) GDPR (legal obligation),
- Art. 6 (1) (f) GDPR (legitimate interest),
- Art. 6 (1) (a) GDPR (consent), if necessary.

6. Location data

Location data is only processed if appropriate functions have been activated.

Insofar as the WebApp processes location data, this is done exclusively:

- after activation of corresponding functions by the user,
- to the extent necessary to provide the functions,
- in compliance with the user's device settings.

The user can deactivate location functions at any time.

7. Recipients of personal data

Data may be transmitted to IT service providers, hosting providers or public authorities.

Personal data may be transferred to the following categories of recipients:

- IT service providers,
- HostingProvider,
- Cloud providers,
- Support service providers,
- affiliated companies,
- Authorities under a legal obligation.

If data is processed outside the European Union, this will only take place in compliance with the legal requirements.

8. Storage period

Personal data will only be stored for as long as it is necessary.

Personal data will only be stored for as long as is necessary for the respective purposes or as long as there are statutory retention obligations.

Once the purpose of processing has ceased to exist, the data will be deleted or anonymised.

9. Cookies and tracking

The web app may use cookies and similar technologies.

The WebApp may use cookies or similar technologies.

These can be:

- technically necessary cookies,
- security cookies,
- Analysis and statisticsCookies,
- Convenience and preferenceCookies.

If required by law, we will obtain consent for this.

10. Analytics and Third-Party Services

The web app can integrate analytics and cloud services from external providers.

The WebApp can integrate services from external providers, such as:

- Web analytics services,
- Maps or location services,
- Cloud infrastructures,
- Push notifications,
- Authentication services.

The specific services used are listed in a supplementary list or in the ConsentManagementTool.

11. Data security

Appropriate technical and organisational measures are used to protect personal data.

We use appropriate technical and organizational measures to protect personal information from loss, tampering, unauthorized access, or disclosure.

These include, in particular:

- encryption,
- role-based access concepts,
- Security logging,

- regular security updates,
- Backup and restore procedures.

12. Rights of Data Subjects

Data subjects have the right to information, correction, deletion and objection.

In particular, data subjects have the following rights:

- Right to information,
- Right to rectification,
- Right to erasure,
- Right to restriction of processing,
- Right to data portability,
- Right to object,
- Right to withdraw consent.

In addition, there is a right to lodge a complaint with a data protection supervisory authority.

13. Changes to the Privacy Policy

We reserve the right to amend this privacy policy if this is necessary due to technical, legal or organizational changes.

The current version is available within the WebApp or on our website.